(12) UK Patent Application (19) GB (11) 2 227 107 (13) A

(43) Date of A publication 18.07.1990

(21) Application No 7934600.3

(22) Date of filing 05.10.1979

(30) Priority data
(31) 7840616 (32) 14.10.1978 (33) GB

(71) Applicant
EMI Limited

(Incorporated in the United Kingdom)

Blyth Road, Hayes, Middlesex, United Kingdom

(72) Inventor
Robert Colin Sloan

(74) Agent and/or Address for Service
R G Marsh
EMI Limited, Blyth Road, Hales, Middlesex UB4 0HB, United Kingdom

(51) INT CL[5]
G06F 12/14

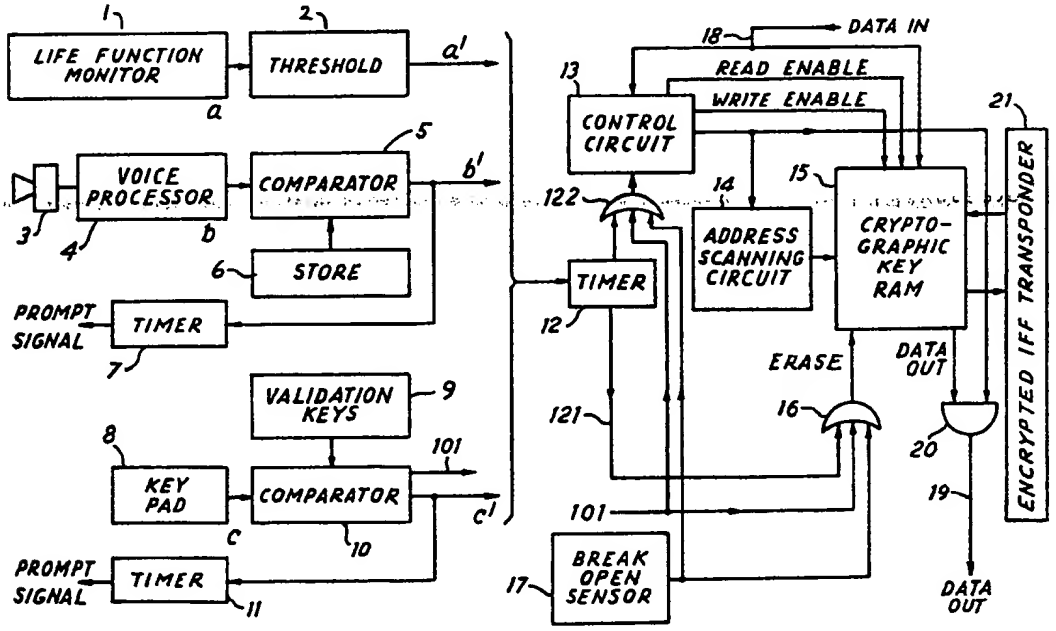
(52) UK CL (Edition K)
G4A AAP

(56) Documents cited
None

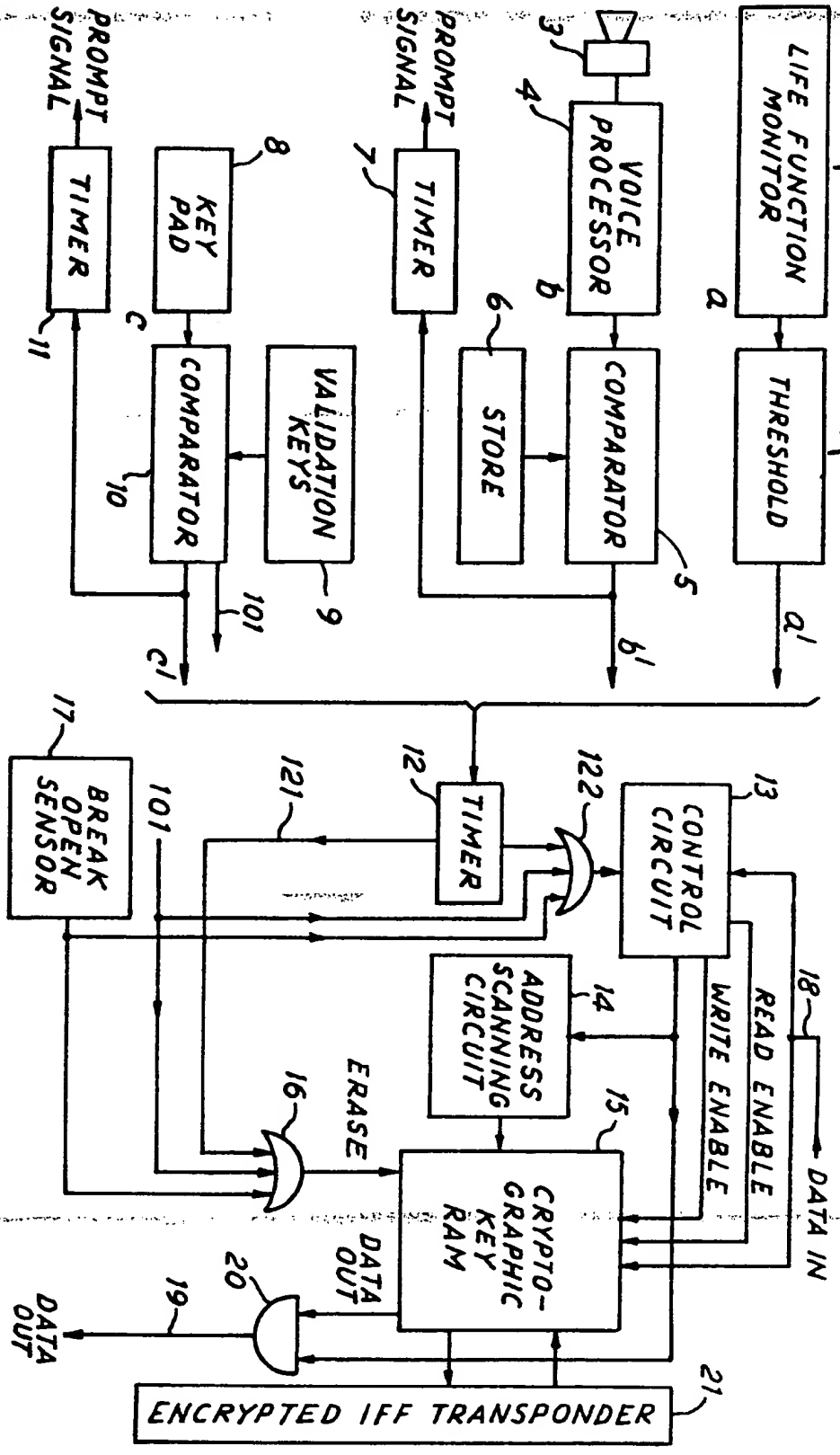
(58) Field of search
UK CL (Edition J) G4A AAP, G4N

(54) Equipment for electronically storing data

(57) In order to make the stored data secure, the equipment comprises one or more sensors (*a*, *b*, *c*) which sense a predetermined characteristic of an authorised user and cause erasure of the stored data if this characteristic is absent e.g. for more than a predetermined time. For example sensor *a* senses a life function such as heart beat, sensor *b* compares a spoken word with a predetermined word spoken by the authorised user, and sensor *c* compares a code with a predetermined code associated with the authorised user. In the case of sensor *a*, a timer 12 causes erasure of data stored in a RAM 15 if the life function is below a threshold level for a preset time. In the case of sensors *b* and *c*, the timer 12 causes erasure of the data if successful comparisons are not regularly performed. In the case of sensor *c* a predetermined number of unsuccessful comparisons causes erasure. Furthermore, a sensor 17 is sensitive to breaking-open of the equipment, to cause erasure of the data.



GB 2 227 107 A


LIFE FUNCTION MONITOR
1
a
THRESHOLD
2
a'
VOICE PROCESSOR
3
4
b
COMPARATOR
5
b'
STORE
6
TIMER
7
PROMPT SIGNAL
KEY PAD
8
c
COMPARATOR
10
VALIDATION KEYS
9
101
c'
TIMER
11
PROMPT SIGNAL
BREAK OPEN SENSOR
17
101
121
12
TIMER
122
CONTROL CIRCUIT
13
ADDRESS SCANNING CIRCUIT
14
WRITE ENABLE
READ ENABLE
18
DATA IN
ERASE
16
15
CRYPTO-GRAPHIC KEY RAM
DATA OUT
20
19
DATA OUT
ENCRYPTED IFF TRANSPONDER
21

EQUIPMENT FOR ELECTRONICALLY STORING DATA

The present invention relates to equipment for electronically storing data.

The techniques of computerised cryptography are now well known so compromisation of the actual hardware configuration used to encode and decode data is of lesser importance than preserving the integrity of the cryptographic keys when these are transported in potentially insecure areas. It is usual procedure for these keys to be changed at predetermined intervals to ensure that there is insufficient time available for the cypher key to be broken during the period of validity; that is, when the key is broken, it will be too late for use with current data. It is, therefore, these keys which need particular safeguarding rather than the actual hardware.

The present invention relates, in a particular application, to military IFF equipment where each operational unit will need to contain the current key plus sufficient succeeding keys to cover the interim period before the next key distribution. Since individual infantrymen armed with missiles such as Blowpipe will each need a valid IFF equipment, this places such equipment in a hazardous position near the front line and highly vulnerable to capture. It is therefore necessary to ensure that an enemy cannot either elicit the current and future IFF keys or make use of an IFF equipment if one is captured intact.

According to the invention there is provided equipment for electronically storing data including means for sensing a

predetermined characteristic associated with an authorised user of the equipment, and means for erasing data stored in the equipment in the absence of the said predetermined characteristic.

The predetermined characteristic may be a life function such as the heartbeat of the autorised user, or a word spoken by the user, or a code associated with the user.

The equipment may be arranged so that the cryptographic keys are erased if the characteristic is absent for more than a preset period of time.

Means may be provided to erase the cryptographic keys if an attempt is made to open or dismantle the equipment.

The equipment may be IFF equipment.

For a better understanding of the present invention, reference will now be made, by way of example, to the accompanying drawing the single figure of which shows an IFF equipment in accordance with the invention including alternative means a, b and c for sensing the presence or absence of the predetermined characteristic. The sensing means a, b or c produces at an output a', b' or c' a sensor signal indicating the presence or absence of the sensed characteristic.

Sensing means a comprises a life function monitor 1 and a threshold circuit 2. The monitor 1 is a transducer for sensing for example the heartbeat of an authorised user of the equipment; other functions could be sensed instead of, or in addition to, heartbeat. The threshold circuit detects, and

produces the sensor signal indicating, the presence of the monitored function such as heartbeat above a predetermined threshold level; this level would not occur if the user is severely wounded or dead. The transducer 1 would be wired to the user and so removal of the equipment from the user would also cause the circuit 2 to fail to detect the function of the required level. Upon failure to detect the monitored function above the threshold level, the cryptographic keys stored in the equipment would be erased, optionally after a short delay, as described hereinafter.

Sensing means b uses voice recognition techniques. The authorised user is required to speak a predetermined word or phrase into a microphone 3 at regular preset intervals.

A voice processor 4 extracts the phonetic features of the spoken word and a comparator 5 compares these features with a set of reference features stored in a store 6. The reference features would be characteristic of only the authorised users voice. A timer 7 is reset whenever the comparator 5 indicates, by production of the sensor signal at output b', that the correct word has been spoken by the authorised user and produces a prompt signal to indicate to the user that the preset interval since he last spoke the word into the processor 4, has nearly ended. If the predetermined word is not spoken into the sensing means b in a manner recognisable by the sensing means b by the required time, the cryptographic keys stored in the equipment will be erased, in the manner described hereinafter.

The store 6 could contain several sets of reference features characteristic of the voices of several authorised users. The sets could represent different words for the respective users or the same word for all the users. An advantage of using voice recognition techniques is that any severe wounding, or physical inducement applied by an enemy to the authorised user to induce him to operate the equipment could change his vocal characteristics in a fail-safe manner. The store 6 could contain a set of phonetic features representing a predetermined self-destruct word. If the self-destruct word is spoken by the authorised user the comparator produces a sensor signal at the output b' causing the erasure of the keys stored in the equipment.

Sensing means c requires the authorised user to enter a validation key at regular preset intervals. It comprises : a keypad 8 for entering the key; a store 9 of validation keys; a comparator 10 for comparing entered and stored keys; and a timer 11. The timer 11 is reset whenever the comparator 10 indicates, by production of the sensor signal at output c, the entry of a correct validation key on the pad 8. The timer produces a prompt signal before the end of the preset interval after that entry to indicate that another entry is required. If a correct entry is not made at the required time the cryptographic keys stored in the IFF equipment are erased in the manner described hereinafter. The comparator 10 could be arranged so that only a strictly limited number of attempts to

enter the correct key may be made. If this number is exceeded the cryptographic keys stored in the IFF equipment would be erased. Any one of the sensing means a, b or c may be used to provide the sensor signal indicating the presence or absence, at the required time, of the characteristic sensed thereby. Two or more of the sensing means could be used together. For instance sensing means a and c could be used together.

The or each sensor signal indicating the presence or absence of the characteristic is fed to a timer 12. In the case of the life function sensing means a, the timer 12 produces an erase signal on its output 121 immediately, or after a short delay from, the sensor signal produced by threshold circuit 2 indicating that the monitored function is below the threshold level; the timer also produces an enabling signal which is fed to a control circuit 13 via an OR gate 122. In the case of the voice sensing means b or the key sensing means c, the timer 12 produces the erase signal on output 121 and an enabling signal which is fed to the control circuit 13 via the OR gate 122 at the end of the present interval from receiving the sensor signal from the comparator 9 and 10 unless it receives a new sensor signal before the end of that interval. The enabling signal causes the control circuit to actuate an address scanning circuit 14 for erasing the keys in the RAM in response to the erase signal. The erase signal produced at output 121 of the timer 12 is fed to an ERASE input of the RAM 15 via an OR gate 16 to erase the cryptographic keys stored in the RAM. The keys may also be erased in response to the IFF equipment being

dismantled or its housing opened as sensed by a sensor 17. For this purpose the sensor 17 produces an ERASE signal which is fed to the RAM via the OR gate 16, and via the OR gate 122 to cause the control circuit 13 to actuate the address scanning circuit. In the case where the key sensing means c is used, the keys stored in the RAM 15 may be erased if the limited number of attempts to enter the correct key is exceeded. In that case, the comparator 10 produces an erase signal on an output 101, which is fed to the ERASE input of the RAM 15 via input 101 of the OR gate 16, and also to the control circuit via the OR gate 122, to actuate the address scanning circuit 14.

It is possible that the keys stored in the RAM 15 are erased, perhaps by accident, and it is necesary to rewrite them into the RAM. As an alternative to returning the equipment to base, provision could be made for a validated functional unit to rewrite the current set of keys in the erased memory. Clearly, the rewriting should be done only if the IFF equipment(s) is/are in the possession of an authorised user(s).

For this purpose the IFF equipment is provided with a databus input 18 and a databus output 19 for receiving keys from, and transfering keys to a similar IFF equipment. It is proposed to transfer the data via fibre optic faceplate couplings to ensure that the exchange is purely local with no possibility of interception. The control circuit enables the input of keys to the RAM 15 or the output of keys from the RAM 15 only if the time 12 has received, within the preset interval, a sensor signal from the sensing means a b or c indicating that

the presence of the predetermined characteristic. In response to that sensor signal and the reception of keys via the data input 18, the control circuit 13 produces a WRITE ENABLE signal enabling the keys to be written into the RAM 15.

Also, in response to that sensor signal the output of data is enabled by the control circuit, which opens an AND gate 20 connecting a DATA OUT output of the RAM 15 to the data output 19 of the IFF equipment.

An encrypted IFF transponder 21 is provided for transmitting data signals encoded by the interrogation keys selected from the RAM 15 and for correlating received encoded data signals with response keys selected from the RAM 15 to decode the received signals.

What we claim is:-

1) Equipment for electronically storing data including means for sensing a predetermined characteristic associated with an authorised user of the equipment, and means for erasing data stored in the equipment in the absence of said predetermined characteristic.

2) Equipment according to Claim 1, wherein the sensing means comprises means for sensing a life function of the authorised user.

3) Equipment according to Claim 2, wherein the life function comprises the heart beat of the authorised user.

4) Equipment according to Claim 1, wherein the erasing means includes timing means arranged to cause the erasure of the stored data unless a signal indicative of the presence of the said characteristic is periodically fed to the timing means by the sensing means.

5) Equipment according to Claim 4, wherein the sensing means comprises means for a spoken word, with a predetermined word spoken by the authorised user.

6) Equipment according to Claim 4 or 5, wherein the sensing means comprises means for comparing a code with a predetermined code associated with the authorised user.

7) Equipment according to Claim 6, wherein the code comparing means is arranged to produce a signal, in response to which the erasing means erases the stored data, after a predetermined number of unsuccessful comparisons of the codes.

8) Equipment according to Claim 4, 5, 6 or 7, wherein sensing means comprises means for sensing a life function of the authorised user.

9) Equipment according to any preceding claim; further comprising a sensor responsive to opening or dismantling of the equipment to cause the erasing means to erase the stored data.

10) Equipment according to any preceding claim in combination with an IFF transponder, the equipment being arranged to store, and supply to the transponder, encryption keys.

11) Equipment for electronically storing data substantially as hereinbefore described with reference to the accompanying drawing.

Published 1990 at The Patent Office, State House, 66 71 High Holborn, London WC1R 4TP. Further copies may be obtained from The Patent Office Sales Branch, St Mary Cray, Orpington, Kent BR5 3RD Printed by Multiplex techniques ltd, St Mary Cray, Kent, Con. 1 87